

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR AN ANTICIPATORY SEARCH WARRANT**

I, Jennifer M. DeMeyer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am currently employed as a member of the West Virginia State Police and have been so employed since September 2009. I have participated in over 250 hours of specialized training in the field of child solicitation and computer forensics. I have personally participated in approximately seventy-five investigations specifically pertaining to child solicitation and/or child pornography. In January of 2016, I was specially appointed as a Special Deputy United States Marshal to perform certain duties as authorized by law, including serving and executing arrest and search warrants supporting a Federal Task Force under Title 18 authority. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

2. On June 2022, I was assigned to the Task Force Officer with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”). I am tasked with investigating violations of state and federal law, such as child exploitation and child pornography, including activity pertaining to the illegal production, receipt, distribution, and possession of child pornography in violation of Title 18 United States Code, Sections 2251, 2252, 2252A, and 2256.

3. I am familiar with the information contained in this affidavit from my personal participation in the investigation, my conversations with other law enforcement officers involved in the investigation, my conversations with other law enforcement officers who have also engaged

in numerous child pornography investigations, and information provided by the National Center for Missing and Exploited Children, and information provided by an HSI Online Covert Employee who conducted an undercover investigation as part of the Child Exploitation Initiative.

4. I submit this affidavit in support of an application for an anticipatory search warrant under Federal Rule of Criminal Procedure 41(b)(1), to search for and seize contraband, evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 2251 (production of child pornography) and 2252A (transport, receipt, distribution, possession, and access with intent to view child pornography) (collectively, the “Subject Offenses”). Specifically, I seek authorization to search for and seize the items more fully set forth in Attachment B of this affidavit.

5. These items are believed to be contained in information associated with the Mega LTD (“Mega”) account lafever234@gmail¹—respectively, the “Subject Account Information” and the “Subject Account.” The Subject Account Information is currently believed to be stored on Mega servers in New Zealand, but is anticipated to be downloaded to computer media in the possession of HSI in the Southern District of West Virginia, as further described in Attachment A.

6. The facts set forth in this affidavit are based upon my investigation, my training and experience, and information I have received from other law enforcement officers and witnesses. Because I am submitting this affidavit for the limited purpose of obtaining a search warrant, I have not included each and every fact I know about this investigation. Instead, I have set forth only the facts that I believe are sufficient to establish probable cause that contraband,

¹ As described in Paragraph 8, a Mega username takes the form of the full email address submitted by the user to create the account.

evidence, fruits, and/or instrumentalities of violations of the Subject Offenses will be located in the Subject Account Information at the time the warrant is executed.

BACKGROUND ON MEGA

7. In my training, experience, and research, I have learned that Mega is a company that provides file-hosting and communications services to the public, through the website Mega.nz. Mega is headquartered at Level 21, Huawei Centre, 120 Albert Street, Auckland, New Zealand. On information and belief, Mega's computer servers are located in New Zealand, and Mega does not have offices or employees in the United States.

8. A Mega user can sign up for an account with a valid email address, which becomes the user's Mega username. Mega provides users with a certain amount of free data storage; if a user wants more storage, the user can pay for it. Users can access Mega through the Internet from most major devices and platforms, from anywhere in the world. For example, a user may take a photo with their cell phone, upload that photo to Mega, and then delete the photo from their cell phone. The photo now resides on Mega's servers. The user can then access their Mega account from a different device, such as a desktop computer, and download the photo to that computer.

9. A Mega user can designate a special folder (or folders) on their computer, which Mega synchronizes with the user's account. As a result, that same folder, with the same contents, will appear on both the user's computer and their Mega account. Files placed in that folder are accessible through Mega's website, as well as its mobile-phone applications.

10. In addition, Mega users can share files with other people by sending web links, which give access to the particular shared files.

11. Another feature of Mega is “MegaChat,” which allows users to exchange messages and hyperlinks and have audio, video, and group chats.

12. According to Mega, data associated with a Mega account is stored on Mega’s servers in an encrypted format. Data is also transmitted in an encrypted format between Mega’s servers and users’ devices. Messages between Mega users are also transmitted in an encrypted format within Mega’s secure server network. Because data is encrypted at all steps, the risk of files or messages being intercepted is minimal.

13. Mega’s server architecture means that data is encrypted in a way that makes it generally inaccessible to Mega. Data is encrypted on the client side using an encryption key to which Mega does not have access. This means that, barring exceptional circumstances, Mega does not have the technical ability to decrypt user’s files or messages and, as a result, Mega is unable to provide data in a usable format to third parties. Mega also is unable to conduct data recovery. If a user forgets their password, Mega cannot recover that user’s data.

14. As explained herein, the Subject Account Information may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This information can indicate who used or controlled the Subject Account. For example, communications, contacts lists, and files sent or uploaded (and the metadata associated with the foregoing, such as date and time) may indicate who used or controlled the Subject Account at a relevant time. The information may also reveal the identity of other victims and the underlying time frames in which they were victimized (e.g., folders with victim data and the metadata associated with file transfers). Additionally, stored

electronic data may provide relevant insight into the Subject Account owner's state of mind as it relates to the offenses under investigation. For example, information in the Subject Account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime) or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

PROBABLE CAUSE

15. On March 20, 2023, your affiant was contacted by HSI Special Agent ("SA") Joshua Knotts regarding the active production of child pornography and hands on sexual assault regarding an adult male and juvenile female. SA Knotts provided your affiant information regarding the incident.

16. On March 16, 2023, HSI SA Dave Alley of Homeland Security Investigations, in an undercover ("UC") capacity, was in chatroom on the KIK messaging application. KIK user thespiderguy2 posted an image that appeared to depict a minor female child from behind, wearing underwear and a shirt. The UC agent contacted KIK user thespiderguy2 and asked about the child in the picture. KIK user thespiderguy2 stated it was his 7-year-old stepdaughter. KIK user thespiderguy2 then sent SA Alley three images: one with this child wearing what appeared to be the same underwear, with her legs spread; one that appeared to be a close-up image of her naked vagina; and one that appeared to depict a finger penetrating the victim's vagina. KIK user thespiderguy2 then sent SA Alley two videos of an adult male hand touching the buttocks of a minor child on top of her clothes and later pulling her shorts away exposing her buttocks. The second video depicts this hand pulling the female juvenile's underwear away from her vagina. KIK

user the thespiderguy2 claims within the conversation to have penetrated this child “a couple of times.” These images and videos appeared to be recorded on an electronic device.

17. On this same date SA Alley sent an emergency disclosure request to KIK to obtain information on the username thespiderguy2. The emergency disclosure KIK return listed Lafever234@outlook.com as the account email address and provided an IP address that had been used to access the account. On this same date SA Alley sent emergency disclosure subpoenas to Frontier Communications for the IP address. Frontier Communications indicated that the IP address had been assigned to Stonerise Healthcare, a nursing home located in Charleston, West Virginia.

18. Based upon this information, SA Knotts was contacted by SA Alley regarding the suspect's location possibly being in the Charleston, Kanawha County, West Virginia area. SA Knotts was forwarded the conversation, videos, and images that were received during the UC chat. In the videos and images, multiple tattoos were clearly visible. One of the visible tattoos was a smiley face with x's for eyes. Open-source searches on the Lafever234@outlook.com returned to a Skype account under the name of Ryan LAFEVER.

19. On March 20, 2023, SA Knotts located a Facebook account of Ryan LAFEVER located in Parkersburg, Wood County, West Virginia. The profile depicted a white male, with tattoos matching those depicted in the videos and images sent throughout the UC chat. An HSI Computer Forensic Analyst also identified the juvenile female depicted in the UC chat videos and images as being linked to the Ryan LAFEVER Facebook page.

20. On this same date, your affiant contacted Lieutenant M. E. Eichhorn of the Parkersburg Police Department in reference to the investigation. Lt. Eichorn advised he was aware

of Jon Ryan LAFEVER, as he was his neighbor. Lt. Eichorn confirmed Jon Ryan LAFEVER's address as being in Parkersburg, West Virginia, and that Jon Ryan LAFEVER lived with his girlfriend and her 6- or 7-year-old juvenile daughter.

21. On this same date, your affiant obtained and executed a state search warrant to search the residence listed above where Jon Ryan LAFEVER resided in Parkersburg. During the execution of the search warrant, eight electronic devices and/or electronic storage devices were seized. During a Mirandized and audio recorded interview with LAFEVER, your affiant learned he utilized Mega to obtain, view, and distribute child pornography. LAFEVER stated his username on Mega was lafever234@gmail.com and provided the password for the Mega account.

22. On March 24, 2023, law enforcement sent a request to Mega for data associated with the Mega account for lafever234@gmail.com (the "Subject Account") to be preserved for future legal request.

23. Mega further provided law enforcement with subscriber and other non-content information regarding to the Mega account for lafever234@gmail.com. This information indicated that the account had been accessed from numerous IP addresses and by numerous devices and browsers.

24. The information in the Subject Account is currently believed to be stored on Mega servers located in New Zealand. It is my understanding that the Fourth Amendment's warrant requirement generally does not apply to locations outside the territorial jurisdiction of the United States, *see United States v. Stokes*, 726 F.3d 880, 890-93 (7th Cir. 2013), and that a warrant issued under Federal Rule of Criminal Procedure 41 would not authorize the search of a server located in New Zealand under these circumstances. *See also United States v. Verdugo-Urquidez*, 494 U.S.

259, 274 (1990) (describing a warrant issued by a United States Magistrate Judge as “a dead letter outside the United States”). Therefore, I seek this warrant out of an abundance of caution, to be certain that an examination of information from the Subject Account (i.e., the Subject Account Information) downloaded to computer media in the possession of HSI in the Southern District of West Virginia will comply with the Fourth Amendment and other applicable laws.

CONDITION REQUIRED PRIOR TO EXECUTION

25. As noted above, in his statement LAFEVER identified the username and password for the Subject Account. Upon information and belief, the information contained in the Subject Account is located on Mega servers in New Zealand.

26. HSI plans on accessing the Subject Account using the credentials identified by LAFEVER; if such access is successful, HSI intends to use Mega’s data transfer tools to download the account’s information onto computer media in the possession of HSI, located in the Southern District of West Virginia. The downloaded information (i.e., the Subject Account Information) may include, but is not limited to, files, communications, and contact lists associated with the Subject Account.


27. I am seeking permission to search the Subject Account Information following the triggering event of the download of said information by HSI into the Southern District of West Virginia, as described in Attachment A, and to seize the items and information described in Attachment B.

28. *Manner of Execution.* Because this warrant seeks permission only to examine information on computer media in law enforcement’s possession, the execution of this warrant

does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

29. Based on the information described above, I respectfully submit there is probable cause to believe that contraband, evidence, fruits, and/or instrumentalities of violations of the Subject Offenses, specifically those items more fully set forth in Attachment B, are currently located in the Subject Account, and will be located in the Subject Account Information in the Southern District of West Virginia at the time the warrant is executed.


Cpl. J. M. DeMeyer
West Virginia State Police
Crimes Against Children Unit
Internet Crimes Against Children Unit
TFO Homeland Security Investigations

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this 22nd day of August, 2023.


DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA